

Queensland State Archives

Managing Emails that are Public Records

**Policy and Guideline for
Queensland Public
Authorities**

Contents

Section One: Introduction.....	2
1.1. Authority	2
1.2. Scope.....	2
Section Two: Policy Principles	3
Meeting Legislative and Regulatory Requirements.....	4
Creating and Capturing Emails that are Public Records	5
Maintaining, Preserving and Disposing of Emails that are Public Records	7
2.4 Providing an Organisational Framework	8
Section Three: Guideline for Applying the Policy Principles.....	10
3.1 Meeting Legislative and Regulatory Requirements	11
3.1.1 Legislative Requirements.....	11
3.1.2 Regulatory Requirements	12
3.1.3 Checklist – Principle 1.....	13
3.2 Creating and Capturing Emails that are Public Records	14
3.2.1 Identifying emails that are public records	14
3.2.2 Creating emails that are public records.....	15
3.2.3 Capturing emails that are public records.....	16
3.2.4 Recordkeeping systems.....	17
3.2.5 Recordkeeping metadata	18
3.2.6 Responsibility for capture.....	19
3.2.7 Assessing the risk of non-capture	21
3.2.8 Checklist – Principle 2.....	22
3.3 Maintaining, Preserving and Disposing of Emails that are Public Records	23
3.3.1 Maintaining accessibility.....	23
3.3.2 Protection of emails that are public records	24
3.3.3 Disposing of emails that are public records.....	25
3.3.4 Checklist - Principle 3.....	26
3.4 Providing an Organisational Framework	27
3.4.1 Support from Chief Executive Officers and shared responsibilities	27
3.4.2 Building the knowledge and capacity of email users.....	29
3.4.3 Email management policies and procedures	30
3.4.4 Checklist – Principle 4.....	31
Appendix A: References	32
Appendix B: Checklists.....	35

Section One: Introduction

Queensland State Archives (QSA) has developed this policy and guideline to assist public authorities to create, capture and manage emails that are public records. This includes emails that provide evidence of a public authority:

- conducting business activities;
- making decisions; or
- carrying out transactions.

Managing emails that are public records presents a number of records management challenges. Unlike paper records, which may be processed through a centralised recordkeeping system, emails can bypass this process.

Consequently, the responsibility for capturing, or initiating capture of, emails that are public records into an identifiable and authorised recordkeeping system has devolved to email users.

Public Authorities are required to comply with the seven principles of *Information Standard 40: Recordkeeping (IS40)* when managing emails that are public records. The additional email-specific principles outlined in this policy should be used by public authorities to develop strategies for creating, managing and retaining emails that are public records for as long as they are required to meet legislative, accountability, business and cultural requirements.

Records and information management specific terms are defined in Queensland State Archives' [Glossary of Archival and Recordkeeping Terms](#), available on Queensland State Archives' website at www.archives.qld.gov.au.

1.1. Authority

The State Archivist has issued this policy in accordance with section 25(1)(f) of the *Public Records Act 2002* (the Act). QSA is responsible for the provision of advisory and support services relating to a wide range of strategic information management and recordkeeping issues for Queensland public authorities. This policy forms one part of a wider framework that aims to promote best practice recordkeeping and information management in Queensland public authorities.

1.2. Scope

This policy applies to all Queensland public authorities as defined in schedule 2 of the Act and pertains to all emails that are public records created or received by a public authority or under contractual agreements by contractors, non-government organisations, shared service providers or Commonwealth agencies.

This guideline provides advice on managing emails that are public records and does not address any other electronic messaging technologies.

Section Two: Policy Principles

Public authorities must:

- 1. Meet all legislative and regulatory requirements relating to the management of emails that are public records***
- 2. Ensure emails that are public records are captured as full and accurate records into an identifiable and authorised recordkeeping system***
- 3. Maintain, preserve and lawfully dispose of emails that are public records, and***
- 4. Provide an organisational framework that supports the management of emails that are public records.***

These policy principles are discussed in more detail in Sections 2.1 – 2.4 of this document, with further information on implementing the policy principles provided in Section 3.

Management of emails that are public records should not occur in isolation from the management of paper-based or electronic records. It should be part an information and records management strategy that encompasses all the information created or received by an authority that is considered the evidence of its business activities.

Meeting Legislative and Regulatory Requirements

Principle 1: Public authorities must meet all legislative and regulatory requirements relating to the management of emails that are public records.

Legislative requirements

Emails that document business activities, decision-making or transactions are public records. Public records must be managed in accordance with the provisions of the [Public Records Act 2002](#).

Public authorities may also be subject to sector or agency-specific legislation that includes recordkeeping provisions. Public authorities may need to seek legal advice or contact Queensland State Archives if additional information or clarification is required.

Table 1 (page 11) provides a brief synopsis of key legislation with recordkeeping provisions that apply to different types of public authorities in Queensland.

Regulatory requirements

Queensland Government Information Standards assist agencies by defining and promoting best practice in information management, information systems and technology infrastructure that support business processes and service delivery.

[Information Standard 40: Recordkeeping](#) (IS40)¹ provides the principles for managing public records in Queensland and is designed to assist public authorities in meeting their recordkeeping obligations under the Act. It includes seven mandatory principles that foster best practice recordkeeping across Queensland's public sector.

Another important information standard relevant to recordkeeping is [Information Standard 31: Retention and Disposal of Public Records](#) (IS31) which complements the retention and disposal requirements in IS40. There are a number of other Information Standards² that are relevant to the making and keeping of public records. Table 2 (Page 13) provides a list of these Information Standards.

Ownership of emails

Section 9 of the *Public Records Act 2002* clarifies ownership of public records. The following provisions, which apply to all emails that are public records, clearly indicate that ownership does not rest with the email sender or receiver.

- Ownership of public records, other than local government records, rests with the State.
- Ownership of local government records in the custody of a local government, rests with that local government.

¹ For further guidance on the meaning, application, scope and implementation of IS40, refer to the [Guideline for Recordkeeping](#).

² Current Information Standards can be accessed from the Queensland Government Chief Information Office website: <http://www.qgcio.qld.gov.au/qgcio/architectureandstandards/informationstandards/current/Pages/index.aspx>

- Ownership of local government records outside the custody of a local government, e.g. in the custody of QSA, lies with the State.

Creating and Capturing Emails that are Public Records

Principle 2: Public authorities must ensure that emails that are public records are captured as full and accurate records into an identifiable and authorised recordkeeping system.

Creating emails that are public records

A public record is recorded information in any format, either created or received, that provides evidence of a public authority carrying out its legislative, administrative or public responsibilities. Public records are a valuable resource and important business assets that support and document decision-making and enable public authorities to conduct business in an orderly, efficient and consistent manner.

As defined in Part 2 of the *Public Records Act 2002*, a public authority is required to create full and accurate records of its activities. This requirement applies to records created in all technological environments including email systems. IS40 describes the attributes of full and accurate records and the recordkeeping processes required to ensure full and accurate records are made.

Capturing emails into a recordkeeping system

Emails that are public records must be captured into an identifiable and authorised recordkeeping system as soon as they are created or received, or as soon as possible thereafter.

An identifiable recordkeeping system encompasses the interaction of people, principles, methods, processes, systems and technology to capture, manage and provide access to records through time.

People

In accordance with Principles 3 and 4 of IS40, responsibility for the management of public records, including emails that are public records, needs to be assigned to managers or senior officers within the public authority. It is their role to contribute to ensuring the public authority creates, maintains, transfers, and disposes of emails that are public records in accordance with the relevant legislation, standards and policies.

Principles, methods and processes

Organisational email policies and procedures that clearly articulate the principles, methods and processes for the capture of emails that are public records should be developed and implemented by all public authorities that use email systems to conduct business. Policy and procedures need to establish responsibilities for capturing emails that are public records and provide clarity on various email scenarios, for example, responsibility for capturing emails that are sent to multiple recipients.

Systems and technology

An authorised recordkeeping system is the system approved by the public authority for the capture, management and preservation of its public records. The recordkeeping system must have the functionality to support and preserve full and accurate records over time, be systematic and have the characteristics of reliability, integrity, compliance and comprehensiveness.

The following systems are NOT considered to be recordkeeping systems:

- Back-up stores of emails within email server systems, on tape backups, in email archives/repositories
- The ad-hoc saving of emails to directories or email folders.

These practices do not meet requirements for the proper capture, accessibility, management, security and disposal of records in accordance with IS40.

Recordkeeping metadata

Recordkeeping metadata is structured information which includes data describing the context, content and management of records through time. As well as enabling the effective management of records, metadata contributes to ensuring that records are full and accurate by documenting the business context of the records creation, and through linking to other related records. Like records in other formats, an email must have content, context and structure to be considered complete.

Recordkeeping metadata is a key tool for ensuring emails are managed as full and accurate records in accordance with the *Public Records Act 2002* and Principle 7 of *Information Standard 40: Recordkeeping*.

Assessing the risk of non-capture

The non-capture of emails that are public records poses a range of risks for public authorities. Public authorities should consider conducting a risk assessment to determine if there are any areas for improvement.

Monitoring or auditing the capture of email over time enables public authorities to evaluate and revise existing email management strategies. Conducting an audit in conjunction with a risk assessment will assist public authorities to prioritise strategies for improvement.

Maintaining, Preserving and Disposing of Emails that are Public Records

Principle 3: Public authorities must maintain, preserve and lawfully dispose of emails that are public records.

Accessibility and preservation of emails

Maintaining and preserving public records over time contributes to a public authority's accountability requirements and ensures ongoing access to the information that is required for the conduct of business.

The failure to maintain and preserve emails that are public records can result in emails becoming inaccessible, which poses a risk to a public authority's requirements to keep full and accurate records.

Public authorities need to develop strategies to ensure that emails that are public records are accessible for their required retention period and that the emails maintain their evidential integrity. This includes strategies to address issues associated with preservation of the email irrespective of whether it is captured in a paper-based or electronic recordkeeping system.

If records are kept electronically, preservation strategies should address issues such as technological obsolescence.

Public authorities also need to ensure that emails are secure from alteration or modification in order to maintain their value as evidence.

Disposal of emails that are public records

Under section 13 of the *Public Records Act 2002*, it is unlawful to dispose of a public record without approval under a Retention and Disposal Schedule authorised by the State Archivist³. *Information Standard 31: Retention and Disposal of Public Records* provides further advice on this issue.

To guard against unlawful disposal, public authorities should ensure that staff are aware of their recordkeeping responsibilities, including the retention periods for public records outlined in approved Retention and Disposal Schedules.

³ A Retention and Disposal Schedule sets out the minimum retention periods for different classes of public records.

2.4 Providing an Organisational Framework

Principle 4: Public authorities must provide an organisational framework that supports the management of emails that are public records.

Shared approach to managing emails

The effective management of emails that are public records requires the coordinated effort, shared responsibility and support of all public authority staff including Chief Executive Officers. Strategic and operational roles and responsibilities should be shared between organisational units, records managers, records staff, Chief Information Officers or equivalent officers, ICT staff, system administrators and individual email system users who create, send and receive emails.

Email management responsibilities

Chief Executive Officers

Overall accountability for recordkeeping, including managing emails that are public records, rests with the public authority's Chief Executive Officer. It is a requirement under Section 7 of the *Public Records Act 2002* that Chief Executive Officers ensure their organisations make and keep full and accurate records of their activities and that they have regard to policies, standards and guidelines issued by the State Archivist under the Act.

To fulfil their responsibilities under the Act, Chief Executive Officers must ensure that recordkeeping systems and the appropriate resources are assigned and processes are in place to achieve recordkeeping compliance.

Email senders and receivers

In many instances, only the person sending an email that is a public record and the person receiving the email are aware that this public record exists. Therefore, all senders and receivers of email have a responsibility to ensure the capture of emails that are public records and contribute to the public authority's recordkeeping obligations. Clarifying the responsibility for the capture of emails that are public records is discussed in section 3.2.6 of the Guideline.

Building the capacity of email users to identify and capture email records appropriately into the public authority's recordkeeping system is integral to successful implementation of email policies and procedures.

Organisational email management policies and procedures

A public authority's formal email policies and procedures are clearly most effective when staff are aware of their existence and there is an organisation-wide commitment to their implementation.

The ongoing development, implementation, monitoring and review of organisational email management policies and procedures that establish rules and document responsibilities for capturing, maintaining and preserving emails will assist a public authority to effectively manage emails that are public records.

Managing emails that are public records needs to be one part of an information and records management strategy that encompasses all the information created or received by a public authority that is evidence of its business activity, including both electronic and non-electronic records.

Section Three: Guideline for Applying the Policy Principles

Email is a critical communication mechanism for Queensland public authorities and a fundamental tool for conducting business. Emails, like public records in other formats, must be captured and appropriately managed to preserve evidence of government activity.

This section provides practical advice on implementing the policy principles discussed in Section 2.

3.1 Meeting Legislative and Regulatory Requirements

Principle 1: Public authorities must meet all legislative and regulatory requirements relating to the management of emails that are public records.

3.1.1 Legislative Requirements

Emails that document business activities, decision-making or transactions are public records and subject to the *Public Records Act 2002* and a range of other legislation containing recordkeeping provisions.

Emails may be subject to administrative and legal processes such as Right to Information, discovery and subpoena. They are potential evidence in civil and criminal cases and may be required to be presented in a court of law.

The following table identifies key legislation with recordkeeping provisions that apply to different types of public authorities in Queensland. Not all legislation listed here may be relevant to every public authority. Public authorities, especially statutory entities and Government-Owned Corporations (GOCs), may choose to seek legal advice on the application of the listed legislation to their operations.

Table 1: Examples of legislation relevant to the management of emails that are public records

Legislation	Purpose
<u>Public Records Act 2002</u>	Aims to ensure that public records are made, managed, kept and, if appropriate, preserved in a useable format for the benefit of present and future generations, and facilitates public access to records in a manner that is consistent with the principles of the <i>Right to Information Act 2009</i> .
<u>Electronic Transactions Act 2001</u>	Framework that supports the use of electronic transactions, subject to some exclusions, and enables business and the community to use electronic communications in their dealing with government.
<u>Evidence Act 1977</u>	Basis for the laws of evidence in Queensland.
<u>Financial Accountability Act 2009</u>	Requirements of financial administration and audit of the State's public finances.
<u>Financial and Performance Management Standard 2009</u>	Subordinate legislation to the <i>Financial Accountability Act 2009</i> . It provides the policies and principles to be observed in financial management within a range of Queensland public authorities. It also provides the authority for the implementation of the mandatory principles of Information Standards.
<u>Right to Information Act 2009</u>	Recognises the right of the community to have access to government documents and to amend personal information held by the government that is not accurate, complete, up-to-date and or misleading.

Legislation	Purpose
<u>Information Privacy Act 2009</u>	Establishes a framework for the responsible collection and handling of personal information in the Queensland Government public sector.
<u>Judicial Review Act 1991</u>	Establishes the right of a court to ask for documents to be produced. Under s54 a court can order that these documents be officially amended.
<u>Public Service Act 2008</u>	Covers the administration of the public service and the management and employment of public service employees, which includes maintaining proper standards in creating, keeping and managing public records.

3.1.2 Regulatory Requirements

Information Standards

Many of the Queensland Government's Information Standards impact on recordkeeping activities in public authorities. [Information Standard 40: Recordkeeping](#) (IS40) and [Information Standard 31: Retention and Disposal of Public Records](#) (IS31) apply to all public authorities covered by the [Public Records Act 2002](#) and should be referred to when developing strategies for managing emails that are public records.

IS40 provides the principles for managing public records in Queensland and is designed to assist public authorities to build systematic recordkeeping into business processes and systems which support business, accountability and cultural requirements. It includes seven principles that are mandatory for the purposes of achieving best practice recordkeeping across Queensland's public sector and includes the requirement for public authorities to keep full and accurate records.

To comply with IS40, public authorities must manage emails that are public records in accordance with the following IS40 principles.

- *Recordkeeping must ensure public authorities are compliant and accountable*
- *Recordkeeping must be monitored and audited for compliance*
- *Recordkeeping activity must be assigned and implemented*
- *Recordkeeping must be managed*
- *Recordkeeping must be reliable and secure*
- *Recordkeeping must be systematic and comprehensive*
- *Full and accurate records must be made and kept for accountability and cultural purposes.*

For further information on the meaning and application of the IS40 principles refer to the *Guideline for Recordkeeping* available at:

<http://www.archives.qld.gov.au/downloads/QGEAGuidelineforrecordkeepingQSA1.0.0.pdf>.

The following table summarises the Information Standards that may apply to different types of public authorities in Queensland and are relevant to the management of emails that are public records.

Table 2: Examples of Information Standards relevant to creating and keeping emails that are public records

Standard	Purpose
<u>IS40: Recordkeeping</u>	Details public authority's obligations under the <i>Public Records Act 2002</i> and fosters best practice recordkeeping.
<u>IS18: Information Security</u>	Provides the mandatory requirements for agencies that are establishing, implementing and maintaining information security within their organisation.
<u>IS31: Retention and Disposal of Public Records</u>	Complements the retention and disposal requirements for government information as described in IS40, the disposal provisions of the <i>Public Records Act 2002</i> and the <i>Financial and Performance Management Standard 2009</i> .
<u>IS34: Metadata</u>	The central standard for the management of metadata schemes for Government information resources.

Australian and International standards

The following international and Australian standards are relevant to managing emails that are public records:

- Australian Standard AS ISO 15489:2002 *Records Management*
- Australian Standard AS/NZS 4360:2004 *Risk Management*.

3.1.3 Checklist – Principle 1

Legislative and regulatory requirements with recordkeeping provisions that apply to the public authority have been identified and documented	<input type="checkbox"/>
The provisions of the <i>Public Records Act 2002</i> have been taken into account in the development of email management strategies within the public authority	<input type="checkbox"/>
The mandatory principles of IS40 have been considered in the development of email management strategies within the public authority	<input type="checkbox"/>
<i>AS ISO 15489:2002 Records Management</i> and <i>AS/NZS 4360:2004 Risk Management</i> have been considered in the development of email management strategies	<input type="checkbox"/>

3.2 *Creating and Capturing Emails that are Public Records*

Principle 2: Public authorities must ensure that emails that are public records are captured as full and accurate records into an identifiable and authorised recordkeeping system.

3.2.1 Identifying emails that are public records

All public authority staff are responsible for creating and initiating the capture of full and accurate records that document the business they transact on behalf of a public authority.

Not all emails are public records. It is important that all public authority staff that create, send or receive emails have the capacity to identify which emails are public records and contribute to ensuring their capture.

There are two main categories of emails that are public records:

1. Business emails
2. Ephemeral emails

Business emails

Emails (including attachments), that provide evidence of the business of the public authority are public records and need to be retained for specified periods of time. Some examples of business emails that are public records are:

- Emails containing business related decisions or information leading to decisions
- Emails containing client or staff records
- Emails relating to business deals i.e. questions about pricing directed to a preferred supplier or an invitation to tender
- Agendas and minutes of meetings with internal or external stakeholders
- Policies and directives, including advice about policy changes and the development of new policies
- Professional advice and guidance provided or received by the public authority
- Emails about work commitments i.e. work schedules and programs
- Emails that initiate, authorise or complete a business transaction
- Final reports or recommendations
- Emails that report incidents e.g. workplace injuries.

Ephemeral emails

Ephemeral emails are of short-term informational value and are only required to be retained for a limited time, usually while they are required for reference purposes. Such emails are not usually incorporated into a recordkeeping system.

Some examples of ephemeral emails include:

- Emails that are duplicate copies of information used only for convenience of reference and not as a public record
- Emails received as part of a distribution list or listserv for information
- Notifications of team meetings
- Spam and unsolicited advertising material.

3.2.2 Creating emails that are public records

Managing emails that are public records begins when they are being created. To be a complete record, an email must have content, context and structure and accurately reflect what was communicated, decided or actioned.

The content of an email is the information contained within the message. This information can either be in the body of the email or within an attachment.

The context of an email includes information about the situation in which the email was created, transmitted and used for the business activity that generated its creation. The context of an email must be maintained if it is to retain its original meaning. The following advice should be taken into consideration when creating an email.

- Ensure that the email subject line is a summary of the document or an action statement and could also contain a file reference e.g. 'Agenda for Corporate Governance Meeting 14/1/2005 - File Ref: ABC1001/05'.
- Avoid using author aliases or 'nicknames' and fancy/decorated borders and backgrounds.
- Include signature and salutation blocks in emails. Details should include, as a minimum, name, title and organisational unit, as this will add valuable contextual information to the message.

The structure of an email refers to its layout (format) and how it relates to the other parts of the message such as links and attachments.

Email style templates or forms will contribute to ensuring that the same structure is applied to all emails.

- Construct emails using style templates or forms that have mandatory fields that assist in bringing structure to email (e.g. a field to categorise emails as: 'business', 'information only' or 'personal', a file reference field, an author signature block etc). Information and technology staff within each public authority can provide advice on designing and implementing email templates.

Table 3: Example of a structured email template

To:	John.Smith@dbus.qld.gov.au
CC:	Records Unit
Subject:	Please provide feedback on Recordkeeping Standard File Ref: GR/POL/003
Message:	<p>John Smith Policy Co-ordinator Policy and Strategy Unit Corporate Services Division Department of Business</p> <p>Hi John Please provide feedback on the exposure draft of the new recordkeeping standard available through the Department of Information website at: http://www.di.qld.gov.au.</p> <p>Responses to the draft should be on the template supplied at the above web address. Completed responses are required by close of business 20/10/08.</p> <p>Regards</p> <p>Jane Jones Senior Policy Officer Strategy & Planning Unit Department of Information Level 1, 2000 Government Street BRISBANE QLD 4000 Telephone: + 61 7 3000 0000 Facsimile: + 61 7 3000 0001 Email: mailto:Jane.jones@di.qld.gov.au URL: http://www.di.qld.gov.au</p>

3.2.3 Capturing emails that are public records

Email systems such as Microsoft Outlook and Lotus Notes are not designed to manage emails that are public records and consequently have limited recordkeeping functionality. Emails need to be captured into an identifiable and authorised recordkeeping system where they can be managed as public records.

In order to be full and accurate records, emails must be captured in such a way that they maintain their context, content and structure. All parts of a message including attachments, links, graphics and sound contribute to context, content and structure.

- Emails that are public records should be captured as soon as possible after the message is sent or received.
- Email systems may be configured to generate an automatic message each time an email is sent (in the form of a pop-up box), prompting email-users to initiate capture of the email if it is a public record. Information technology staff can provide advice on configuring this functionality if the public authority decides to implement this approach.

- Before any email is deleted from an email system, a decision needs to be made about its status as a public record and if appropriate its capture into a recordkeeping system.
- Systematic deletion of emails when a mailbox reaches a certain size or after a period of time exposes the public authority to the risk of unlawful disposal of public records.
- Messages from IT system administrators to staff requesting that public authority staff delete emails to free up space on drives should be accompanied with a reminder that emails that are public records need to be captured in the public authority's recordkeeping system.

Business classification schemes and thesauri, based on a public authority's functions and activities, assist in the integrated and consistent management of records, including emails. Thesauri create a controlled vocabulary for categorising and indexing files and public records. Examples are *Keyword AAA: A Thesaurus of General Terms* and *Keyword for Councils*. Contact Queensland State Archives for information about gaining a licence to use these thesauri.

- Emails that are public records should be captured into a recordkeeping system and filed according to a business classification scheme and thesauri.
- A unique number should identify each email that is captured into a recordkeeping system. Public authorities should determine a protocol for this. It may be generated by the records unit when the email is registered as a record or generated when the email is moved from the email system to an Electronic Document and Records Management System.

3.2.4 Recordkeeping systems

Emails can be captured in different formats depending on the public authority's recordkeeping system. They can be captured in electronic form in an Electronic Document and Records Management System (eDRMS). In situations where a public authority does not have an eDRMS, emails can be printed and filed in a paper-based recordkeeping system.

Electronic Document and Records Management Systems

Electronic Document and Records Management Systems facilitate a number of fundamental recordkeeping processes including classification and appraisal, while also ensuring the authenticity and reliability of electronic records.

Public authorities may wish to consider the DIRKS (Designing and Implementing Recordkeeping Systems) methodology for the design and implementation of an eDRMS. The DIRKS manual provides advice to agencies with a step-by-step implementation process for systems that will support both recordkeeping and business requirements.⁴

⁴ National Archives of Australia (2003) *The DIRKS Manual: A strategic approach to managing business information*. Available <http://www.naa.gov.au/records-management/publications/dirks-manual.aspx>

Paper-based recordkeeping systems

When an eDRMS is not available, emails and appropriate contextual detail can be printed to paper and filed into a paper-based recordkeeping system. The evidential value of the email is protected if metadata, such as transmission and receipt data (i.e. time sent and received), is included in the printed version.

Records management staff should liaise with information and technology staff to ensure appropriate email metadata can be printed with emails that are public records.

3.2.5 Recordkeeping metadata

Recordkeeping metadata describes the context, management, use, and preservation and disposal action of records. Attaching recordkeeping metadata to emails that are public records allows them to be located, controlled and managed appropriately and ensures context is maintained.

In the email environment, as for other records, the capture and maintenance of recordkeeping metadata in accordance with an approved recordkeeping metadata standard is essential to the quality of “completeness” in relation to a public record.

Metadata includes descriptive information such as author, recipient and date/time of transmission as well as information about the business context (e.g. the business function and activity that generated the record), a meaningful and relevant file number, and management information (such as its retention and disposal status).

Depending on a range of factors such as the functionality of the email system and integration with a recordkeeping system, some metadata may be system-generated (e.g. date and time of transmission), some may be created while authoring the email (e.g. names of recipient and full details of sender) and some may be manually generated when capturing the record into a recordkeeping system. The following table outlines some of the information that is required as recordkeeping metadata⁵, and at what point this information is usually created and captured for emails.

⁵ This is not a complete list: for more information on mandatory metadata see Queensland State Archives' *Queensland Recordkeeping Metadata Standard and Guideline*.

Table 4: Examples of recordkeeping metadata

Metadata	Capturing the metadata
Record Title	May be based on the subject line of the email (if the subject line is meaningful)
Date	Automatically generated by system
Agent – author / recipient	Included in body of email, and also captured when the email is registered into a recordkeeping system May also include the email address, which can be captured from the To/From fields in the email header
Classification / business function	Inherited from the parent file when the email is captured in a recordkeeping system
Disposal	Inherited from the parent file when the email is captured in a recordkeeping system
Access / security	Inherited from the parent file when the email is captured in a recordkeeping system

[Information Standard 34: Metadata](#) (IS34) requires Queensland public authorities to apply metadata schemes that are interoperable with the Australian Standard 5044 “AGLS Metadata Element Set”. However, AGLS is a resource discovery metadata standard and the use of this standard is not sufficient to ensure that email is managed as full and accurate records⁶.

3.2.6 Responsibility for capture

Responsibility for capturing emails needs to be assigned and consistently applied. An internal email policy or corporate procedure should outline that emails that are public records are captured into the recordkeeping system (not stored in folders in the email system or on network drives) and outline staff responsibilities for ensuring this occurs.

The following information outlines two issues that need to be considered in managing the capture of emails that are public records.

Responsibility for initiating capture

In many instances, only the person sending an email that is a public record and the person receiving the email are aware that a public record has been created. Therefore, all senders and receivers of email have a responsibility to at least initiate the capture of emails that are public records, if not the actual capture itself (discussed in the next section). As mentioned in 3.2.1, staff should be aware that ephemeral emails do not usually need to be captured.

⁶ For more information on the relationship between IS34, AGLS and recordkeeping metadata contact Queensland State Archives.

When assigning responsibility to email senders and receivers for initiating capture of email that are public records, some options to consider are:

- The sender initiates capture when an email is sent to either single or multiple internal or external recipients.
- The email recipient initiates capture when:
 - the email relates to their work
 - they are involved in the business transaction to which the email relates
 - the email is from an external sender.

An internal protocol for capturing emails that have been received by multiple recipients from an external sender needs to be determined by each public authority. Options include:

- The recipient who is most directly involved in the business transaction or has designated responsibility for the issues, task or project initiates capture, or
- The first person on the receiving list initiates capture.

Responsibility for capture

Once capture is initiated, the actual capture can be assigned to either the public authority's Records Unit, or to an email sender or receiver.

If the Record's Unit is responsible for capture, the following must occur:

- Staff who receive emails that are public records forward a copy of the email to the Records Unit for capture.
- All outgoing emails that are public records are copied (CC:) to the Records Unit by the sender for capture into a recordkeeping system.
- Completed email threads (i.e. a record of an email dialogue) are forwarded to the Records Unit for capture once they are complete.
- The emails should contain a file reference number to assist the Records Unit with capture and classification.

If email senders or receivers are responsible for the actual capture, they must be appropriately trained in the use of the recordkeeping system and fundamental recordkeeping principles.

Capturing attachments

If the recordkeeping system is paper-based, attachments should be printed out and captured with the covering email.

If emails are sent with attached documents that have already been captured in the recordkeeping system (particularly if it is an eDRMS,) it may not be necessary to capture the attached document again.

- In these circumstances, a reference or link to the location or the attachment within the recordkeeping system may be sufficient. Public authorities may choose to capture both the email and the attachment as one record or a two separate but related records.
- If there is a possibility that the link may change over time rendering the attachment inaccessible then the best approach would be to capture the attachment with the email.

Capturing the email thread

Emails that are public records should be captured as soon as they are sent or received or as soon as possible thereafter. However, emails often involve a thread of communication that can continue for a period of time. Public authorities should determine and implement a corporate approach for the timing for capturing emails.

Options may include:

- Capturing each email as it is sent or received. As capture becomes a routine component of the business process, the risk of non-capture of records is reduced; however this option may increase storage requirements.
- Capturing at the very end of the communication thread. This may increase the risk of non-capture of the record into the recordkeeping system, as the end of the thread may not always be apparent.
- Capturing at significant points throughout the communication thread, where key decisions are made, subjects change, or key issues addressed.

3.2.7 Assessing the risk of non-capture

Non-capture of emails that are public records poses a range of legal and other risks for public authorities. These risks need to be considered when determining a strategy for addressing email management issues.

- Conducting a risk assessment will help public authorities to identify, assess and report on risks relating to the non-capture of emails that are public records, and to plan appropriate risk mitigation strategies for improving overall email management processes.
- Risk factors relating to accountability, accessibility, protection and disposal of emails are discussed in Section 2.3 of this guideline.

Further guidance on risk assessment can also be found in the Australian Standard AS/NZS 4360-2004 *Risk Management*.

The DIRKS manual has a short appendix on risk analysis at:

http://www.naa.gov.au/Images/dirks_A11_risk_tcm2-939.pdf and step C of the manual suggests identifying recordkeeping requirements and assessing the risks associated with these. http://www.naa.gov.au/Images/dirks_stepC_tcm2-960.pdf.

Monitoring email capture

The monitoring or auditing of email capture enables public authorities to evaluate and revise existing email management strategies and to establish a culture of continuous improvement. Some methods for monitoring email capture are:

- Auditing the number of emails being registered into the recordkeeping system
- Auditing corporate files to determine if emails have been attached
- Interviewing or surveying staff regarding business conducted by email to identify emails that should have been captured.

Conducting an audit in conjunction with a risk assessment will assist public authorities to identify areas for improvement.

When addressing issues of non-capture it is important to ensure that current systems are capable of implementing the processes for capturing emails that are public records. New systems or work processes may need to be introduced to support and promote capture of emails that are public records.

3.2.8 Checklist – Principle 2

All employees and contractors are aware of their responsibilities for creating and capturing full and accurate records of business they conduct by email	<input type="checkbox"/>
All employees and contractors have the capacity to identify and initiate the capture of emails that are public records	<input type="checkbox"/>
Procedures for the creation and capture of emails that are public records have been developed and implemented	<input type="checkbox"/>
The recordkeeping system has been designed and implemented in a way that allows the capture of emails that are public records	<input type="checkbox"/>
Recordkeeping metadata is being created and captured with emails that are public records	<input type="checkbox"/>
A risk assessment has been conducted prior to the development of email management strategies	<input type="checkbox"/>
Email capture is monitored and email management strategies revised to address areas of risk	<input type="checkbox"/>

3.3 Maintaining, Preserving and Disposing of Emails that are Public Records

Principle 3: Public authorities must maintain, preserve and lawfully dispose of emails that are public records.

3.3.1 Maintaining accessibility

Emails that are public records must be maintained in a readily accessible, useable and meaningful format, irrespective of the origin or format of the records. For example, it is not sufficient for emails to be stored on system backup tapes which are at risk of technical obsolescence and require time-consuming searches to retrieve information.

Accessibility of emails in email systems

Email systems generally only allow the creator and the recipient to access an email. The accessibility of an email is significantly reduced or non-existent if it has not been captured into a recordkeeping system. Ideally, capture should occur when the email is sent or received, or as soon as possible afterwards (see Section 2.2, Creating and Capturing Emails that are Public Records).

Storage of emails that are public records in an email system can be particularly problematic when a public authority staff member, contractor or other people employed for a business activity cease employment. There is a risk that emails may not have been transferred from an individual's mailbox to the recordkeeping system, rendering them inaccessible.

- The ideal situation is that emails that are public records are captured into the recordkeeping system when they are sent or received.
- If necessary, procedures should be implemented to ensure that all emails are appraised and those that are public records transferred from the email system to the recordkeeping system when a public authority staff member ceases employment.
- One strategy is to ensure that the checklist for departing employees includes a category regarding the capture of emails (i.e. 'all emails that are public records have been captured into the recordkeeping system or forwarded to the Records Unit for capture into the recordkeeping system').

Migration strategies

If emails that are public records are captured in an electronic format, public authorities should consider the following issues:

1. longevity of file formats used
2. storage media lifespan and obsolescence, and
3. maintaining the integrity of data.

Public authorities should develop strategies that address these issues to ensure emails captured as electronic records remain accessible for their required retention periods and that the original content, structure and context of the email is retained.

Generally, to preserve electronic records designated for long-term retention, media and formats need migration across successive software and hardware platforms.

Migration policies and processes should be documented as part of a public authority's overall information management plan.

Managing legacy emails

Managing a back log of emails (legacy emails) that have been stored either in individual email inboxes or on system backup tapes can be challenging for public authorities.

- If required, public authorities should develop strategies to address issues relating to legacy emails. Planning should include determining priority areas and assigning responsibility for identifying legacy emails that are public records and capturing them into the recordkeeping system, as well as securing sufficient resources to undertake the task.
- Assess the relative priority level of each business area based on:
 - the function of the emails that they receive or create and the level of relevance to the public authority's core business
 - the level of risk of recordkeeping non-compliance by various units
 - the retention requirements of the emails
 - the proportion of business emails that are of short-term value only.
- Develop strategies for the identification of emails that are public records and their capture into the recordkeeping system based on staff knowledge and the available resources within each business unit.

3.3.2 Protection of emails that are public records

In order to maintain their value as evidence, emails are to be inviolate. They are not to be altered or manipulated during any phase of their transmission, capture or storage. If alteration is unavoidable during a migration process for preservation purposes, it must be strictly controlled and documented to ensure that the content and metadata associated with the email are not lost.

- Recordkeeping systems, procedures and practices must protect emails that are public records at all times from accidental or deliberate alteration or deletion as well as inappropriate access.
- Capturing and maintaining emails in a format that enables the email to be accessed in the form in which it was originally represented will retain the evidential integrity value of the email.

- Embedded links to other resources and attached files containing documents, graphics, video, images also need to be protected wherever possible to ensure the value of the record is retained.
- Arrangements for managing emails should operate in accordance with policies that apply to the management of all records and protect personal privacy (in accordance with the *Information Privacy Act 2009*), confidentiality or commercially sensitive information from unauthorised access, disclosure, manipulation, improper concealment, deletion or removal.
- Access to recordkeeping and business systems with recordkeeping functionality should be controlled through the use of a range of security measures such as passwords, user names and security classifications schemes.
- Physical access to emails that are public records stored in paper-based recordkeeping systems should also be controlled and monitored.
- Public authority staff should be aware that alteration of the content of public records including emails that are public records can only occur where legislation allows it. (e.g. some provisions of the *Information Privacy Act 2009*).
- Scanned images of signatures should not be included in emails that are public records as they may be misused and do not add to the authenticity of the email.

3.3.3 Disposing of emails that are public records

Under section 13 of the *Public Records Act 2002*, it is unlawful to dispose of a public record except under an approved Retention and Disposal Schedule authorised by the State Archivist. Disposal includes destroying or damaging a record or part of it and abandoning, transferring, donating, giving away or selling a record or part of a record.

Unlawful disposal of public records is an offence punishable by a fine of 165 penalty units. The QSA and Crime and Misconduct Commission publication: *Managing Public Records Responsibly* available at <http://www.cmc.qld.gov.au/data/portal/00000005/content/57402001156128645546.pdf> provides more information regarding the unlawful disposal of public records.

In addition to the *General Retention and Disposal Schedule for Administrative Records*, all Queensland public authorities are required to have a schedule that relates to their specific operations and outlines the periods of time for which records must be kept.

- Emails that are public records must not be deleted without first consulting the public authority's Retention and Disposal Schedule approved by the State Archivist.
- Emails that are public records should be retained in accordance with retention requirements set out in an approved Retention and Disposal Schedule with disposal documented in accordance with Information Standard 31: *Retention and Disposal of Public Records*.

- Public authorities should develop internal procedures for the disposal of emails that are public records and include the requirement for approval from the Records Unit or the individual with delegated authority for disposal.
- Emails that are ephemeral records according to Section 6 of the General Retention and Disposal Schedule for Administrative Records may be deleted when no longer needed without a requirement for capture into a recordkeeping system. Appropriate and timely disposal of ephemeral records should be part of a public authority's normal administrative practice.
- Original emails that are business records may be deleted from user inboxes after they have been captured into an identifiable and authorised recordkeeping system.
- Regular and appropriate capture of emails that are public records and disposal of other emails should take place to avoid overloading email systems resulting in possible unplanned or indiscriminate deletion of records by email users and system administrators.
- Care should be taken when implementing any systems or functionality which may interfere with authorised disposal processes. For example, the Document Rights Management functionality available in some email systems can allow email users to set an 'expiry' date for an email, potentially giving rise to unauthorised disposal. Such practices should be avoided.

3.3.4 Checklist - Principle 3

A migration program for emails captured as electronic records has been developed and implemented where necessary	<input type="checkbox"/>
Emails that are public records are transferred from the email system to the recordkeeping system as they are sent or received	<input type="checkbox"/>
A strategy for addressing legacy emails has been developed and implemented where necessary	<input type="checkbox"/>
Information security protocols and procedures have been developed, implemented and maintained to ensure emails remain inviolate	<input type="checkbox"/>
Approved Retention and Disposal Schedules are applied to manage the disposal of emails that are public records	<input type="checkbox"/>

3.4 Providing an Organisational Framework

Principle 4: Public authorities must provide an organisational framework that supports the management of emails that are public records.

3.4.1 Support from Chief Executive Officers and shared responsibilities

The effective management of emails that are public records requires the coordinated efforts and sharing of responsibilities between individuals involved directly or indirectly with all stages of the email management process. This includes organisational units, records units, Chief Information Officers or equivalent officers, ICT staff or system administrators and individuals who create, send and receive email.

Chief Executive Officer support and the provision of adequate resources are essential if a public authority is to successfully manage emails that are public records. Chief Executive Officers have a responsibility under Section 7 of the *Public Records Act 2002* (the Act) to ensure that their agencies make and keep full and accurate records of their activities. To fulfil their responsibilities, Chief Executive Officers must ensure that:

- the public authority creates full and accurate records of its activities
- the public authority has regard to policies, standards and guidelines issued under the Act
- recordkeeping responsibilities within the public authority are assigned
- recordkeeping systems and processes are in place and are appropriately resourced
- A positive recordkeeping culture is actively promoted and supported throughout the public authority.

The development and implementation of email management strategies is most successful in an environment in which there is an effective working relationship between senior management, records and information managers and information technology specialists.

Larger public authorities may wish to establish internal working groups involving staff such as chief information officers, records managers, information technology specialists or system administrators to assist in the coordination of email management strategies and associated issues.

While there may be different or merged roles and responsibilities assigned to individuals involved in the coordination, administration and management of emails that are public records, they can generally be distinguished according the following table:

Table 5: Suggested Email Management Roles and Responsibilities

Position	Responsibilities
Chief Information Officer or equivalent officer	<ul style="list-style-type: none">• Accountable for overseeing and coordinating the information management and/or information technology activities of the public authority
Email system administrators or information technology specialists	<ul style="list-style-type: none">• Maintain the email system technology and monitor system reliability• Implement appropriate security and protection measures for email systems• Manage controls of the email system including the regular backing up of the system and its data• Manage the volume of emails in the system
Records manager or equivalent officer	<ul style="list-style-type: none">• Provide advice and assist in the development and implementation of policies, procedures and tools for managing emails• Contribute to the provision of email management training• Monitor the capture and maintenance of emails that are public records• Capture of emails that are public records into the recordkeeping system• Monitor and conduct the disposal of emails according to approved Retention and Disposal Schedules
Workgroup managers	<ul style="list-style-type: none">• Ensure staff under their supervision understand and comply with email management policies and procedures• Support and foster a culture within their workgroups that promotes the effective management of emails that are public records
Senders and receivers of emails	<ul style="list-style-type: none">• Comply with email management policies and procedures• Determine if emails are public records and capture them, or initiate their capture with the associated metadata into the public authority's authorised recordkeeping system

3.4.2 Building the knowledge and capacity of email users

Building the knowledge and capacity of email users to manage emails that are public records is essential if a public authority is to meet its recordkeeping obligations successfully.

There are several issues to address in terms of capacity – awareness, attitude and skills. Staff need to be aware of their recordkeeping responsibilities; they need to accept their recordkeeping responsibilities; and they need to have the skills to carry out these responsibilities.

Raising **awareness** can be achieved in a number of ways. Some examples are the provision of information at team meetings and inductions or a basic training course to provide information (rather than provide skills).

Gaining **acceptance** from staff that they have certain recordkeeping responsibilities may present a challenge for some public authorities. These challenges can be addressed through a range of change management initiatives, such as:

- Explaining the need for email users to perform recordkeeping activities
- The provision of information (oral and written) about recordkeeping responsibilities
- The provision of basic training to demonstrate how the recordkeeping responsibilities would be carried out
- Ongoing access to a forum for email users to communicate concerns and issues
- Identification of email management champions
- Establishment of a temporary change management officer within the Records Unit to assist email users with change strategies
- “Cheat sheets” – desk-top ready reference tools to assist users.

The **knowledge and skills** staff will need to perform their recordkeeping responsibilities will depend on the operational environment and the public authority’s recordkeeping system. However, some of the knowledge and skills required include:

- Being able to identify emails that are public records
- Knowing how to capture an email into an eDRMS (or other recordkeeping system)
- Basic understanding of the agency’s Business Classification Scheme and Retention and Disposal Schedule.

Staff can gain the knowledge and skills required through the provision of information and appropriate training. Some examples are:

- Provision of electronic access to email management policies and procedures (e.g. via an intranet)
- Information and training at induction sessions

- Training in email management for existing employees (e.g. online or group sessions)
- Presentations on email management requirements at staff briefings and meetings.

Queensland State Archives online training module

Queensland State Archives in conjunction with TAFE Queensland has developed an online training module for all public authority staff which aims to provide them with an understanding of their responsibilities for managing emails that are public records.

This module can be used as a training tool during an induction course for new staff and delivered to existing staff to ensure that they are aware of their recordkeeping obligations. The module is available at

http://www.archives.qld.gov.au/learning/email_module/email_home.html.

3.4.3 Email management policies and procedures

The management of emails that are public records needs to be supported by a broader information and records management strategy that encompasses all the information created or received by a public authority that is evidence of its business activity, including both paper-based and electronic records.

However, the development and implementation of corporate policies and procedures for specifically managing emails that are public records should be undertaken by public authorities.

Corporate policies and guidelines for managing emails that are public records should include information regarding:

- Legislative and regulatory obligations
- The broader corporate information and recordkeeping policy and strategy
- Responsibilities for determining the value of emails that are public records
- Process for capturing emails that are public records into the recordkeeping system
- Responsibilities for the retention and disposal of emails that are public records
- Security, access and conditions of use of the email system
- Structuring emails to ensure that recordkeeping metadata is captured
- Organisational guidelines for capturing emails attachments, email threads and those sent and received by multiple recipients.

3.4.4 Checklist – Principle 4

The Chief Executive supports the email management strategy and has ensured sufficient resources for its implementation	<input type="checkbox"/>
The appropriate level of awareness raising and training for staff using email has been identified and undertaken	<input type="checkbox"/>
All staff using email are aware of and understand the public authority's email management policies and procedures	<input type="checkbox"/>
The public authority's broader information and records management plans include email management	<input type="checkbox"/>
Recordkeeping roles and responsibilities have been identified and documented in email management policies and procedures	<input type="checkbox"/>

Appendix A: References

Legislation

Public Records Act 2002 (Qld.). Available online:

<http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/P/PublicRecA02.pdf>. Accessed 10 January 2007.

Electronic Transactions Act 2001. Available online:

<http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/E/ElectronTrQA01.pdf> Accessed 10 January 2007.

Evidence Act 1977. Available online:

<http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/E/EvidceA77.pdf> Accessed 10 January 2007.

Financial Accountability Act 2009. Available online at:

<http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/F/FinAccountA09.pdf>. Accessed 14 August 2009.

Financial and Performance Management Standard 2009. Available online at:

<http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/F/FinAccPManSt09.pdf>. Accessed 14 August 2009.

Information Privacy Act 2009. Available online at:

<http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/InfoPrivA09.pdf>. Accessed 14 August 2009.

Judicial Review Act 1991. Available online at:

<http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/J/JudicialRevA91.pdf>. Accessed 10 January 2007.

Public Service Act 2008. Available online:

<http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/P/PublicServA08.pdf>. Accessed 14 August 2007.

Right to Information Act 2009. Available online at:

<http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/R/RightInfoA09.pdf>. Accessed 14 August 2009.

Standards and Toolkits

AS ISO 15489.1 (2002) *Records management - General*. Available from Standards Australia,

<http://www.standards.com.au>

AS ISO 15489.2 (2002) *Records management - Guidelines*. Available from Standards Australia,

<http://www.standards.com.au>

AS/NZS 4360:2004: *Risk Management*. Available from Standards Australia.

<http://www.standards.com.au>

Guideline to Recordkeeping. Available online:

<http://www.archives.qld.gov.au/downloads/QGEAGuidelineforrecordkeepingQSA1.0.0.pdf>. Accessed 10 January 2007.

Information Standard 18: Information Security. Available online:

<http://www.qgcio.qld.gov.au/qgcio/architectureandstandards/informationstandards/current/Pages/index.aspx>. Accessed 14 August 2009.

Information Standard 31: Retention and disposal of Public Records. Available online:

<http://www.qgcio.qld.gov.au/qgcio/architectureandstandards/informationstandards/current/Pages/index.aspx>. Accessed 14 August 2009.

Information Standard 34: Metadata. Available online:

<http://www.qgcio.qld.gov.au/qgcio/architectureandstandards/informationstandards/current/Pages/index.aspx>. Accessed 14 August 2009.

Information Standard 40: Recordkeeping. Available online: <http://www.qgcio.qld.gov.au/qgcio/architectureandstandards/informationstandards/current/Pages/index.aspx>. Accessed 14 August 2009.

National Archives of Australia, *DIRKS Manual – Glossary*. Available online: http://www.naa.gov.au/Images/dirks_glossary_tcm2-954.pdf. Accessed 10 January 2007.

National Archives of Australia *Recordkeeping Metadata Standard for Commonwealth Agencies*. Available online: <http://www.naa.gov.au/records-management/publications/RKMS.aspx>. Accessed 10 January 2007.

Email Management Policies and Guidelines

State Records NSW (1998) *Policy on electronic messages as Records*. Available online: <http://www.records.nsw.gov.au/recordkeeping/government-recordkeeping-manual/documents/recordkeeping-policies/Policy%20on%20Electronic%20Messages%20as%20Records.pdf> Accessed 10 January 2007.

National Archives of Australia (NAA) (1997) *Managing Electronic Messages as Records*. Available online: <http://www.naa.gov.au/records-management/systems/email/index.aspx> Accessed 10 January 2007.

State Records of South Australia (2002) *Management of Email as Official Records*. Available online: http://www.archives.sa.gov.au/files/management_guidelines_managementemail.pdf. Accessed 12 January 2007.

Archives Office of Tasmania (2005) *Managing Email as Records*. Available online: http://www.archives.tas.gov.au/legislative/staterecords/guidelines_list/guideline_07. Accessed 10 January 2007.

Public Records Office of Victoria (PROV) (2002) *Emails as Records: Advice to Victorian Government Agencies*. Available online: <http://www.prov.vic.gov.au/publications/publIns/PROVRMadvice3.pdf>. Accessed 10 January 2007.

Archives New Zealand (2006) *Fact sheet: E-mail*. Available online: <http://www.archives.govt.nz/continuum/documents/publications/factsheets/f10.php>. Accessed 10 January 2007.

UK National Archives (2004) *Guidelines for developing a policy for managing Email*. Available online: http://www.nationalarchives.gov.uk/documents/managing_emails.pdf. Accessed 10 January 2007.

eDavid project (2006), funded by the Flemish Government, Belgium *Filing and archiving email*. Available online: http://www.expertisecentrumdavid.be/docs/filingArchiving_email.pdf. Accessed 10 January 2007.

Library and Archives Canada (2006) *Email Management in the Government of Canada*. Available online: <http://www.collectionscanada.ca/information-management/002/007002-3008-e.html>. Accessed 10 January 2007.

Government of Alberta, Canada (2005) *Managing Electronic Mail in the Government of Alberta*. Available online: <http://www.im.gov.ab.ca/publications/pdf/ManagingEmailGuide.pdf>. Accessed 10 January 2007.

Kentucky Department for Libraries and Archives (2003) *Guidelines for Managing Email in Kentucky Government*. Available online: <http://www.kdla.ky.gov/recmanagement/EmailGuidelines.pdf>. Accessed 10 January 2007.

Nebraska Government (2003) *Electronic Messaging and Electronic Mail (email) Guidelines*. Available online: http://www.sos.state.ne.us/admin/record_manage/pdf/guideline_e_mail_march_2003.pdf. Accessed 10 January 2007.

New York State Archives (2002) *Managing E-Mail Effectively*. Available online: http://www.archives.nysed.gov/altformats/ServicesGovRecs/ns_serv_mg_pub62.pdf Accessed 10 January 2006.

Other Information

Queensland State Archives (2004) *Glossary of Archival and Recordkeeping Terms*. Available online: <http://www.archives.qld.gov.au/downloads/GlossaryOfArchivalRKTerms.pdf>.

Appendix B: Checklists

Checklists for Implementing the Policy Principles

Principle 1: Public authorities must meet all legislative and regulatory requirements relating to the management of emails that are public records.

Legislative and regulatory requirements with recordkeeping provisions that apply to the public authority have been identified and documented	<input type="checkbox"/>
The provisions of the <i>Public Records Act 2002</i> have been taken into account in the development of email management strategies within the public authority	<input type="checkbox"/>
The mandatory principles of IS40 have been considered in the development of email management strategies within the public authority	<input type="checkbox"/>
<i>AS ISO 15489:2002 Records Management</i> and <i>AS/NZS 4360:2004 Risk Management</i> have been considered in the development of email management strategies	<input type="checkbox"/>

Principle 2: Public authorities must ensure that emails that are public records are captured as full and accurate records into an identifiable and authorised recordkeeping system.

All employees and contractors are aware of their responsibilities for creating and capturing full and accurate records of business they conduct by email	<input type="checkbox"/>
All employees and contractors have the capacity to identify and initiate the capture of emails that are public records	<input type="checkbox"/>
Procedures for the creation and capture of emails that are public records have been developed and implemented	<input type="checkbox"/>
The recordkeeping system has been designed and implemented in a way that allows the capture of emails that are public records	<input type="checkbox"/>
Recordkeeping metadata is being created and captured with emails that are public records	<input type="checkbox"/>
A risk assessment has been conducted prior to the development of email management strategies	<input type="checkbox"/>
Email capture is monitored and email management strategies revised to address areas of risk	<input type="checkbox"/>

Principle 3: Public authorities must maintain, preserve and lawfully dispose of emails that are public records.

A migration program for emails captured as electronic records has been developed and implemented where necessary	<input type="checkbox"/>
Emails that are public records are transferred from the email system to the recordkeeping system as they are sent or received	<input type="checkbox"/>
A strategy for addressing legacy emails has been developed and implemented where necessary	<input type="checkbox"/>
Information security protocols and procedures have been developed, implemented and maintained to ensure emails remain inviolate	<input type="checkbox"/>
Approved Retention and Disposal Schedules are applied to manage the disposal of emails that are public records	<input type="checkbox"/>

Principle 4: Public authorities must provide an organisational framework that supports the management of emails that are public records.

The Chief Executive supports the email management strategy and has ensured sufficient resources for its implementation	<input type="checkbox"/>
The appropriate level of awareness raising and training for staff using email has been identified and undertaken	<input type="checkbox"/>
All staff using email are aware of and understand the public authority's email management policies and procedures	<input type="checkbox"/>
The public authority's broader information and records management plans include email management	<input type="checkbox"/>
Recordkeeping roles and responsibilities have been identified and documented in email management policies and procedures	<input type="checkbox"/>

Contact Details

If you have any queries about this policy and guideline please contact:

Policy and Research Unit
Queensland State Archives

Phone: (07) 3131 7777

Fax: (07) 3131 7764

Email: info@archives.qld.gov.au

Physical Address: 435 Compton Road Runcorn Qld 4113

Mailing Address: PO Box 1397 Sunnybank Hills Qld 4109

Website: <http://www.archives.qld.gov.au>